

Configuración de reenvío de DNS del equilibrador de carga F5 para acceso seguro

Contenido

Problema

La resolución de DNS no funcionaba cuando se utilizaba un equilibrador de carga F5 como servidor DNS del cliente durante la migración de Umbrella a Secure Access. Cuando las solicitudes de DNS llegan a la IP virtual (VIP), el equilibrador de carga F5 reenvía correctamente los paquetes a los reenviadores DNS de backend, pero los nombres de host no se resuelven en las máquinas de terminales. La resolución DNS funcionó correctamente cuando se utilizó un dispositivo virtual directamente como servidor DNS del cliente, lo que indica que el problema era específico de la configuración del equilibrador de carga F5.

Las capturas de paquetes revelaron que las respuestas DNS estaban utilizando la dirección IP del dispositivo virtual en lugar de la dirección VIP F5 esperada. El equipo cliente esperaba que las respuestas DNS provengan de la dirección VIP F5 , pero en su lugar recibió respuestas de la dirección IP del dispositivo virtual backend.

Entorno

- Entorno de migración de Cisco Umbrella to Secure Access
- Equilibrador de carga F5 con VIP de equilibrio de carga DNS configurado
- Varios reenviadores DNS como servidores backend
- Dispositivos virtuales que actúan como servidores DNS
- Terminales de cliente que requieren resolución DNS a través del equilibrador de carga

Resolución

El problema se resolvió configurando el equilibrador de carga F5 para que actuara correctamente como proxy entre los equipos cliente y los dispositivos virtuales. El cambio de configuración clave implicaba habilitar la Traducción de direcciones de red de origen (SNAT) con la funcionalidad de asignación automática.

Pasos de diagnóstico realizados

Paso 1: Verificar el comportamiento de resolución DNS

La resolución de DNS se ha probado utilizando tanto la conexión VIP del equilibrador de carga F5 como las conexiones de dispositivos virtuales directos para aislar el problema.

Paso 2: Capturar y analizar el tráfico DNS

Las capturas de paquetes se realizaron para analizar el flujo de solicitud y respuesta de DNS a través del equilibrador de carga F5.

Paso 3: Identificar discrepancia de dirección de origen

El análisis reveló que las respuestas DNS contenían la dirección IP del dispositivo virtual en lugar de la dirección VIP F5, lo que causaba confusión en el cliente.

Cambio en la configuración

Paso 1: Acceder a la configuración del equilibrador de carga F5

Vaya a la interfaz de administración del equilibrador de carga F5 para modificar la configuración VIP de DNS.

Paso 2: Habilitar mapa automático de SNAT

Configure SNAT (traducción de direcciones de red de origen) para asignar automáticamente en el equilibrador de carga F5. Esto garantiza que el dispositivo F5 realiza correctamente el proxy de las solicitudes y respuestas DNS entre los clientes y los servidores DNS backend.

Paso 3: Verifique la configuración

Después de implementar la configuración de mapa automático SNAT, la resolución DNS comenzó a funcionar correctamente a través del equilibrador de carga F5.

Causa

La causa raíz fue una configuración incorrecta de la traducción de direcciones de red de origen (SNAT) en el equilibrador de carga F5. Sin SNAT auto-map habilitado, el dispositivo F5 no estaba actuando correctamente como proxy para el tráfico DNS. Esto hacía que las respuestas DNS se enviaran directamente desde los dispositivos virtuales de back-end a los equipos cliente, utilizando la dirección IP del dispositivo virtual como origen en lugar de la dirección VIP F5 esperada. Los equipos cliente esperaban que las respuestas DNS se originaran en la misma dirección IP a la que enviaron sus solicitudes (el VIP F5), pero recibían respuestas de direcciones IP diferentes (los servidores de administración), lo que provocaba errores en la resolución DNS.

Contenido relacionado

- [Configurar el equilibrio de carga de F5 GTM](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).